Policing and Use of Information Technology: An Assessment

by

Dr. Marcel-Eugène LeBeuf

Research Centre
Canadian Police College
Ottawa, 2000

101-01408/

Introduction

Currently, the police have to deal with a new paradigm. They have seen the gradual end of one period where, for many years, they had full control over their field of action, to a period, which is not transitory, where three new factors are to be observed simultaneously: technology-based criminal activity that has none of the characteristics of traditional crime; new high-performance working tools that require very specialized training for their use; a stronger articulation by the public at large as to the role they wish the police to play within their environment.

This document provides a summary of the various issues and problems related to the introduction and use of information technologies within the public security. It also takes into account the upsurge in a new type of criminal activity that makes use of technology and that has abandoned traditional means of the past. It examine avenues that will allow law enforcement bodies to prepare for the technological future, something they have hardly begun to do (Tafoya, 1995).

The very expression 'Information Technology' is ambiguous, general and yet restrictive. The term is used to designate a variety of more or less complex gadgets, machines and software which, as Nogala (1993) put it, have each their own specific development, use and impact. The term 'Information Technology' leads us to ask two basic questions which, though easy to express, are difficult to answer: Which of these technologies are useful to our police forces? How does the integration of such technologies change the role and task of the police?

In this document, we are looking at the development of information technology as it effects public safety. Without attempting an exhaustive overview, we will be looking at a number of key elements of these technologies, including, without priority ranking:

- information technology and the police
- integration of the technologies into the traditional police environment
- equipping the police with MIS
- technology users within a police department
- introducing technological tools
- incentives and de-incentives
- the cost of technologies
- the impact of technologies on police operations
- IT training
- ethics and liability

Information Technology and the Police

The interaction between the police and technology is complex rather than linear. It concerns both power and information. With respect to power, information technology promotes actions and secure results that were previously impossible to achieve, and thus police operations are improved (Manning, 1992). Moreover, the public image of the police and their impact on society are significantly enhanced. To this end, the Web pages published by police departments constitute an innovative exercise in public relations which allows them to inform the public of crime prevention activities in their locality, supply statistics on the level of criminality and provide an information framework with regard to missing persons (Strandberg, 1998; Haley, Taylor, 1998; Goodman, 1997; Wilsker, 1997; Anderson, 1997; Corsentino, Pettinari, 1996).

With regard to the information to which the police have access, it is true to say that technology allows the police to remain a symbol of authority within communities (Ericson, Haggerty, 1997). This is because such access, to data banks and other computerized instruments, provides them with more information and thus allows them to develop more effective strategies for combatting both traditional and high-tech crime (McLean-Lipinski, 1999). As police work, to use Manning's (1992) expression, is ecologically scattered, its sought-after effectiveness depends on a number of factors including the organizational culture of the various groups of workers, the type of information that is stored and the methods of doing so. Information

warfare is a real threat and includes money laundering, gaming, all forms of extortion including credit cards or the use of computers to falsify data, economic crimes, MIS sabotage, computer hacking, spying and other activities by groups linked to organized crime (Coutorie, 1995; Dobeck, 1997; Carter, Katz, 1998). Committing such crimes do not depend on geographic movement. Real crime and real issues are to be found in a new virtual universe which is now well established (Rosé, 1996). The new connections are horizontal and invisible (Marx, 1997). To win in this universe, you have to be the one holding the joystick. If law enforcement bodies hope to be as smart as the criminals, they will need to adopt the technological tools available on the market (Campbell, 1997). The challenge is not so much to adopt information technology as to adapt information technology that can systematically be helpful to the police in dealing with these new problems and issues.

Integration of the Technologies into the Traditional Police Environment

It is relatively difficult to chart the current use of technologies by the police. Technology has been part of the police environment for more than 150 years (Soullière, 1999). However, to date it would seem that, as a whole, this technology has been used in a transient and sporadic manner in a number of police departments across Canada. In fact, they have been aware of the utility of technologies for more than fifteen years (Carpenter, 1984). However, the technology sector market has developed at a speed that is in inverse proportion to that of public police department decision making. The police represent a potential market and one that needs to be developed rapidly. This means that the police need to learn how to determine both their own needs and those of the community they serve in order to make an informed choice of the most appropriate technological tool.

It is a well known fact that within police departments, the decision makers do not always have the skills required to make the necessary decisions (Carpenter, 1984) or even to become involved in decision-making (MacDonald; Martin, 1986) within a process whose ramifications have become less and less transparent (Loree, 1987). When it comes to information technology, the situation is even more complex, since the decision makers deal with new tools that can be very effective when properly used, but which are perfectly foreign to the traditional police environment (Martin, 1996).

In many cases, there are a number of new elements: the technology as such (e.g. AFIS—Automated Fingerprint Identification System), the link between technology and traditional work, and the ability to fully exploit this technology. During our research project, we visited a certain number of police departments. On one occasion, a police officer demonstrated the crime mapping system. At some point, the police officer admitted that she had taken more than eight months to learn how to handle the software, which clearly would have given much better results than those she obtained, if she had received the appropriate coaching and had some level of skill in data management.

This example shows that technological tools can be very effective if they have been developed specifically for the police or in cooperation with the police. The performance of these tools would appear to be a relative matter since the amount of extra information obtained through the use of the software will depend on whether or not the user is capable of fully exploiting its potential. Most of us who have used word processing software such as *Word Perfect* or *Word* will recall that they only discovered the fine points in these applications after several years of daily use. The performance of any apparatus will vary according to the way in which the user exploits it. However, one should not forget that all software has built-in restrictions that come into play when integrated into a larger technological whole.

Equipping the Police with MIS

New technologies will put a fresh face on the services offered in order to meet the needs of the tax payer (Audet et al.,1996). They will contribute to transforming the police into a body that is truly at the service of the citizens, a community police force, as it were. The population looks at the money that is pumped into the public domain and demands a higher level of performance from the services they are supporting (LeBeuf, 1998). But the need of the users, in this case the police, must also be met as they gradually

move from being a traditional reactive force and become a more pro-active service. To deal with this problem, the Sûreté du Québec (community relations activities) has developed a reference tool, the ARC project, that records every police intervention within the framework of crime prevention.

To meet client needs, the organizations have set up intelligence structures that allow the police to intervene rapidly, effectively and autonomously in their local neighbourhoods. Currently, a number of police departments are equipped with technology such as the AFIS (Automated Fingerprint Identification System) for fingerprinting, or the GPS (global positioning system) for communications, or even mobile data computers. We still need to construct a more detailed chart of the situation of the police forces on a country-wide basis. We should also mention that, internally, the relationship between superiors and subordinates is changing, thanks to the new level of autonomy acquired and experienced by employees who have more direct access to data banks and, consequently, to the potential for strategy updates.

However, the private security market, which is innovative and primarily concerned with the protection of property, has developed and uses tools that are often well ahead of any system that public security organizations can afford. It won't be long now, certainly not a question of decades, before the major areas of protection, whether of places, property or persons, will be ensured not by human beings, but by robotics, satellites, nanotechnology and micro-engineering (Moore, 1995; Akrich, Méadel, 1993). Moore (1995:2) describes security zones that can now be protected by invisible movement-sensitive light rays or by laser or pulsers. Robotics has also an exceptional role to play in laboratories, thanks to the delicate handling operations which it allows when, for example, extracting chemical compounds (Johnson, 1997). Biometrics, a technology which brings together finger prints, palm prints, specific features of the face, and readings of the retina or the iris, will constitute the future identification system. In the same way, DNA (deoxyribonucleid acid) identification will become commonplace. Indeed, the Canadian Parliament has adopted the *DNA Identification Act* that authorizes the setting up of a DNA data bank for genetic identification of persons convicted of serious crimes.

Technology Users within a Police Department

There are as many technology users in a police department as there are tasks to be accomplished. It is not the same person who uses a crime mapping system or a mobile data computer. In the first case, it is the analysts who have access to the software and whose task it is to obtain as much information as possible for the benefit of investigators and of patrol officers. But investigators and patrol officers themselves do not have either direct or even limited access to this tool. In the second case, however, the patrol officers deal with the information directly in their patrol car. They access the material that allows them to work better and which simplifies their tasks often by getting rid of all the paper work.

Overall, and this will simplify our demonstration, we could classify users into four main types: the executive, the investigator, the patrol officer and partners. However, one should remember that any form of discrete classification also eliminates the complex aspects of the demonstration.

Senior executives, or those in charge of teams, are looking at a lessening of financial and human resources. They will be required to look to improved technologies in order to carry out their tasks in a different manner (Morrison, 1996). But executives have been trained in their work with methods from another era and in a pre-technological environment (Rodriguez, 1995). Today, they have to articulate their needs using their own understanding of technological tools, by taking a technological standpoint that corresponds to the strategic and corporate vision of their organization. They need to create flexible organizational structures to manage both the work and the individuals, to encourage horizontal cooperation between the units and, most of all, to understand and control a decision-making process based on skills and not on rank (Martin, 1996).

Moreover, the organized crime or computer crime unit investigator is now required to understand and use new tools to deal with the challenges of this type of criminality. Henceforth, investigators, search warrant in hand, are less likely to confiscate ledgers or other pre-MIS documents. They will be looking for PCs and hard disks, and will be intercepting encrypted cell phone communications. In other words, they will be dealing with the world of communication technology that affects society as a whole, but which is also used for criminal activity.

Analysts, for their part, can now access an enormous number of data banks that offer material for their work. How can they make a proper choice of material, taking into account the needs to be met? One of the first consequences of accessing such a vast amount of material is that analysts must learn to think differently. Rather than concentrating on a single problem, they will need to develop the ability to think up several problems and several possible solutions at the same time, and sometimes collaborate with colleagues scattered across the world, whose experience and language are different from theirs (Dorn, 1998). Like everyone else, analysts find themselves faced with too much information. Data will have no significance unless it is transformed into a language that is meaningful for operations and/or management. These new tools necessarily change our ways of looking at crime and analyzing it. The VICLAS (violent crime linkage analysis system), for example, which is used in the case of serial murders, totally changes the investigators' use of their accumulated data (Sheptycki, 1998). Could unlimited technology become a hindrance for the police because of the difficulty in processing it all?

Depending on their department, patrol officers are now using patrol cars that have been transformed into mobile MIS laboratories. On the one hand, a number of boring repetitive tasks have been simplified thanks to data banks and software. Nevertheless, patrol officers still learn to manage and coordinate the technology on board, whether it be the camera that photographs them when they leave their car, the mobile data terminal, lap-top, or the mobile data computer, E-mail and so many other tools. These items improve police safety and police performance (Parsons, 1993). It is believed (LeBeuf, 1999) that tomorrow's patrol officers will be community based. This remains to be seen, but they will certainly be technology-based.

Moreover, since information technology generally eliminates a certain number of tasks, one could imagine that there will be a sense of collegiality and cooperation between colleagues and MIS specialists. As we have already mentioned, we need to get these specialists out of their offices and encourage them to cooperate with police officers in order to adapt technology to their needs. The MUCPD engineer in charge of developing MIS has insisted that front-line police officers should be involved in his work structure so that the systems developed meet their needs.

However, contrary to what is generally thought, technology confines individuals even more closely within the perimeters of their tasks, demanding a high level of competency and the development of a cutting-edge skill. Once analysts have learned to handle crime-mapping software, for example, they will begin to discover the full potential of the tool. In other words, individuals achieve a high level of performance not so much as police officers, but as experts in the management of a piece of software. This restructuring of their working approach leads them to understand and define the reality of crime in its full complexity, thus eliminating simplistic explanations (Catalyst, 1996). If you transfer such individuals, then you will create new training costs and, more especially, an indecisive period where the analysis of criminality will not be carried out at the same level of competency as previously.

Finally, we must look at another category of users, who have a very specific relationship with technologists. We are talking here of industry and government which themselves may be involved in partnerships with the police. Reports of various experiments in US partnerships of this kind indicate the advantages for the police of cooperating with major private industries (Fulton, 1995), or with government services such as the army (Smietan, Ferris, 1996; Preimsberger, 1996). Research into non-lethal weapons has had major impact on police work, giving rise to technologies such as the *smart gun* or the *sticky foam* (a spray that immobilizes a dangerous suspect), the *road patriot* (which stops a vehicle by disconnecting its electrical system), imagery process mirrors (developed by space researchers to significantly enhance blurred or inaccurate images), and the *GPS* that provides patrol car latitude and longitude and allows them to be located rapidly. The Collines-de-l'Outaouais Regional County Municipality police department, that operates over a vast rural area, uses this technology to provide a greater margin of safety for its personnel.

Another form of partnership is based on the possibility of exchanging information between the police and community groups through the use of a more effective information system (Catalyst, 1996). The premise is that the police is not the sole depository of information concerning life within the community, and constructive exchanges can easily be envisaged through the use of various technologies. The question still remains as to how to ensure that the use of technologies enhances the ability to systematically diagnose social problems (Sloan, 1996).

We should avoid making hasty generalizations at a time when the police forces are often still learning by trial and error how to handle instruments that are new to them and that were not included in their original job-training process.

Introducing Technological Tools

At the beginning of the 1990s, a major police department decided to adopt the new forensic identification technology. The process, which lasted five years, allowed the implementation of the AFIS and eliminated a great number of forms and documents from the files. This was the beginning of the paperless era. However, these five years of major change had their ups and downs. The operation had been planned out on paper, but a certain number of major problems developed during the process of change: suppliers went bankrupt; certain data bases could not be activated because of incompatible platforms; the systems sometimes went down while manual data contained in files was being transferred to computerized data banks, arousing a great deal of critical comment. Finally, the destruction of old files led to extremely violent reactions from the employees whose handwritten notes were destroyed. Once the process was completed, the system required only two work stations compared with the previous twenty-eight.

Consequently, one of the major difficulties faced by the executive is to develop a business plan to meet the daily needs of the process. However well change is planned out, it will not give good results if it does not take into account simultaneously the development of tools, of mentalities and of the factor of resistance to change. Technology is handled by men and women exposed to diverse levels of stress because of their police work, and because of the professional framework in which they operate. The degree to which the hoped-for results of technological innovation are achieved will depend as much on one as on the other factor.

Moreover, the introduction of MIS also requires the ability to take in experts to look after the running of the system for the short or medium term. It is quite fascinating to note that police departments have taken in experts from computer companies or have created positions for civilians, computer engineers, computer technicians, etc. to ensure the proper management, planning and replacement strategies related to the new systems. The new creative spirit within the police department (Pitcher, 1995) is the computer technician or technology manager. The police, consequently, is welcoming highly qualified specialists, not so much as managers of scientific areas such as laboratories, but rather in order to plan out and develop advanced computer programs for their whole staff (for example, mobile data computers) (Breton, 1996).

It happens that the product offered by a company does not correspond exactly to the needs of the police. We should then look at developing, along with the company, a product that does meet these needs. As we were told, Aif a product does not exist, we will have it made, but that supposes an enormous level of involvement. This, however, is not the role of the police, but of researchers who, aware of the complexity of police work, set out to design new tools. The role of the police is to adapt the appropriate technology to its own needs. With this new strategy in mind, we will call on the police to cooperate with experts rather than to play the role of experts themselves, as they do traditionally. This means that the police will adapt their normal work methods on the basis of their own ability to handle the high-performance tools available to them. It should be noted that, although their tasks will be refined and simplified by technology, the final result may not be greatly enhanced. New technologies do not create competence or experience.

Incentives and Disincentives

How does one make it easier for a police organization to adopt a technological approach? Nogala (1993) identifies the internal and external incentives and de-incentives. Let us take a look at them.

Internal incentives result from factors at different levels. One, for example, is the improvement of performance in the application of the law and in cooperation between police departments. The incentive may be to combat major banditry, day-to-day criminality and the fast developing area of technological crime. It is in this last area that we find the new types of crime linked to the use of technology, an area which is still difficult for the police departments to handle. Consequently, the orientations or strategies favoured by the police will promote and accelerate the use of technology and integrate it more and more

into the system as a whole. There are essential conditions to be met in order to do this, including the ability to pay for the technology and the ability to integrate it into the working environment. It will also be necessary to strengthen cooperation between police forces, cooperation which may, for example, involve the use of special squads, like *Carcajou*, which was set up to combat organized motorcycle gangs in the Montreal area in the mid-nineties and which brought together police officers from the Sûreté du Québec, the MUCPD and the RCMP. Cooperation of this kind facilitates rapid exchanges, adequate communication and information sharing. We still need to assess how, in fact, the information exchange process works, particularly where information technology is not compatible.

There is a second, rather different factor involved. The police are involved in a definitive professionalization and specialization process. Investigators dealing with organized crime have had to add to their working tools the use of the ACIIS II, an automated criminal intelligence information system, which allows them to identify the position and role of criminals within organized crime (Kerr, 1999b). The introduction and full use of cutting-edge technology require that the users have highly specialized technical qualifications. Should we, therefore, train personnel on-site so that they can fully exploit the potential of these technologies or should we bring in experts who not only can handle the technology, but can also monitor the rapid process of changes in the area? More generally, the issue is the strategic vision to be developed by police departments, in order to meet the needs of their communities and of the members of their departments. They must also be able to make informed decisions as to the technologies they select, so that such technologies do not become obsolete too rapidly.

A third factor worth bringing out is that these new technologies appear to be effective weapons of incredible potential. For example, the *compstat*, following its initial testing out by the New York police department (Bratton, Nobler, 1998) has developed into a strategic tool for neighbourhood crime management and has also helped project an image of the police force as being active both in prevention and repression (Green Mazerolle, Haas, 1998). It has got to the point where advanced seminars are being held on just this subject. This means that the police are perceived as able to solve more problems and to maintain their power of social control through the use of technologies placed at the service of the community (National Institute of Justice, 1997).

External incentives are linked to technological progress and rapid social development. One of the new and irresistible driving forces is the incredible speed with which both current and developing technologies are changing (Castells, 1996). The innovative cycle has become very short, equipment has become more powerful and cheaper, as complex processes are transformed into day-to-day tools. After two or three years, an MIS is often out of date or no longer compatible with other computerized systems that have been acquired since the initial installation. This means that police departments are likely to find themselves faced with one or more of four problems: they may be overtaken by the technological market; they may lag behind the most recent developments; they may be hindered in their development by the fact that their systems are no longer compatible, or they may be unable to expand because they lack the financial resources to upgrade the systems they do have. The technological market is knocking on the public security door, having first saturated the private security market which, as we have already mentioned, is less and less people-dependent (Moore, 1995). Moreover, the security needs of individuals and private commercial interests had led to a search for technological solutions to security problems (Boullier, 1993; Clarke, 1993). The development and introduction of video surveillance is no longer exclusive to private security, but has become a working tool for public security services as well (Ocqueteau, Pottier, 1993).

Disincentives to progress are numerous and relate to several factors concurrently. As of now, the police will be using more and more sophisticated and costly equipment. However, there is a clear gap between what we hear from engineers and specialists and the daily experience of police users. Technology does not always carry out its promises and sometimes makes only a slight difference. In fact, if we can make a simple analogy, having a word processor isn't enough to make you a writer. Technology becomes effective when a certain number of ideal conditions are met, such as proper training, backing by experts, in-depth knowledge of the use of the apparatus. Sometimes technology only becomes really useful after expensive adaptations.

Another important and determining factor is the limits of police financial resources. It is not possible to finance all the desirable technical options and all the products available on the market. Direct and indirect

costs are high and recurrent. The purchase of an apparatus now means that in the relatively short term, i.e. after a few years, it will be necessary to change or to upgrade it. Likewise, the development, research and maintenance of technological skills are relatively costly for the police, which means that even today these technologies are often not seen or perceived as a priority. Moreover, since it is necessary to develop and adapt training for each change in the technologies used by the police, immediate and direct costs ensue. The police have moved into the era of permanent and ongoing change.

Another important aspect of the changes created by technology, which is proving to be a major and complex obstacle, is the situation of the police forces around the country. According to the Canadian Constitution, police forces, with the exception of the RCMP, come under the jurisdiction of the provinces. This means that there is a fragmentation of the overall police entity that is difficult to deal with when trying to develop national standards. Moreover, the various police departments tend to go their own ways and don't have a natural impulse to get together in order to create a critical mass, for the purchase of material, for example. This means that it is very difficult to ensure compatibility of the technologies that have been developed by different companies. Finally, small and medium-sized police departments do not have regular on-staff experts who can assess the technologies, the aappropriateness of purchasing and ensure strategic planning of the technology to be acquired (Brady, 1996).

The Cost of Technologies

It is difficult to determine the direct cost of technologies. Do these costs only cover the apparatus or the software, or should they also include costs linked to personnel training, to the restructuring of human resources and system security?

There are recurrent costs related to the purchase and upgrading of apparatus and technological tools of all sorts. And budgets should take these into consideration. Then there are hidden costs linked to the introduction of the technology. They include the expense of recurrent or prolonged sick leave taken by individuals who resist change or wish to sabotage it. Another problem is that of demotivation and apathy, factors that are more difficult to evaluate, but are nevertheless significant and which can contribute to the costly failure of a technological venture.

Another cost factor is the training of both personnel and senior executives. Though the issues and training costs may be complementary, they are nevertheless different. It is indeed astonishing that there is so little literature regarding the training of top-level executives within the field of information technology or on the type of information required for the development of a strategic vision and an informed decision. However, training is a constant priority and subject to continuous upgrading. Tomorrow's training programs must be developed bearing in mind the concerns and needs of tomorrow. Again, a wider vision is needed to compass the new issues raised by technology.

Finally, technology security itself raises significant and costly problems B problems to be resolved and problems to be eliminated. If there is a general consensus that information technology substantially enhances the effectiveness and performance of police users, what is perhaps less well known is that, as we shall see later on, the same technology increases public vulnerability (Grabosky, et al., 1996). Examples of this vulnerability are the development of new crimes such as telemarketing fraud, embezzlement of electronic transfers, illegal tapping of cell phones and electronic vandalism. In the latter case, we refer to a virus attacking the MIS in the same way that viruses attack human beings. It costs an enormous amount of money, not only to protect oneself against illegal attacks and invasions, but also to reboot the weakened or destroyed system (EDP Security Bulletin, 1998).

The Impact of Technology on Police Operations

The impact of technology on police operations is various and varies according to the sectors concerned. The opening hypothesis is that technology is integrated into police work on the basis of the benefits that they will engender for police operations. This hypothesis remains to be proved. Within the information technology sector in particular, one can identify three major forms of impact.

Recourse to technology increases the effectiveness of one's work by eliminating or reducing the number of repetitive tasks, in particular for patrol officers. This leads to an improvement in performance, more rapid response time and a higher solution rate (Seaskate, 1998, Lingerfelt, 1996). By transferring some part of the administrative tasks of the police officer to civilian personnel, patrol officers have more time to devote to their community. Again, in the field of forensic identification, the fact that one can access computerized files that already contain basic information, significantly reduces the time needed to complete electronic forms. There are less repetitive actions required. Moreover, the information obtained is of higher quality, since police officers can immediately check out the data banks and, where necessary, fill in missing information.

Technology opens the door to the installation of an extended communication network which has a high performance level and interconnects departments that otherwise would not be in touch. However, one still has to assess the quality of these contacts and the results obtained by the new network. An analyst working in a major police department reports that she was able to contact a large number of analysts and investigators in her department thanks to E-mail and the Internet. However, she also noticed that if she used the telephone, she was able to develop stronger and more personal relationships, which worked in her favour when it came to long-term information exchanges and cooperation. Direct person-to-person contact meets the need to set up a real network of more humane contacts and thus to obtain more accurate and specific information. A more superficial contact created by E-mail comes in handy when you need only general factual information.

The setting up of high performance (or significant) communication networks has an immediate ripple effect which modifies decision-making practices. It means that a police department that wishes to tie in with a powerful high-performance system needs to have equipment that is compatible with that used in other departments or in the major regional departments. The transfer of information and knowledge collated in data banks is more and more dependent on the transfer of technology. From this point of view, information technology generates improvements in working techniques, but it does not replace them.

When police officers work with information technology, there is less emphasis on the evaluation of the task in terms of performance or quantitative results than on the ability to work through different sites with multiple connections. New work divisions are based on the capacities and skills of the worker rather than on the task. For example, forensic identification teams are now much smaller, but their work is completed more rapidly and more accurately, with fewer personnel. Police officers in the forensic identification program do not inevitably work faster than formerly. This is not necessarily what is asked of them, but the Identification Section offers more effective overall results since a large number of repetitive tasks no longer need to be effected thanks to the inception of computerized data banks.

IT Training

Police training has been transformed with the introduction of technology. Not only is there a prime need to train people in the use of this technology, but technology itself is used to provide training. Here we are referring to the development of distance training (Wells, Minor, 1998). Staff are trained in accordance with their needs and using electronic contacts including Internet (Myers, Myers, 1998) and at some future date intranet (Kerr, 1999). Individuals may access teleconferencing or training programs assisted by computers or CD-ROM (Hutchison et al. 1998), or make use of firing range or driving simulators to allow learners to experience situations that are as close to reality as possible (Pilant, 1994). One Canadian experiment in the training field is *Athabaska University*, a virtual university which has no campus but trains students.

We have referred several times to the needs for training to be priorized within the fundamentally changing context of police work and technology. Indeed, technology means that apparatus and data banks are more powerful, that the ability to swap information has been multiplied ten times and that interconnections between the systems, police departments and data banks are easier to make than ever.

The inevitable question is whether technology is creating a new police profession. If so, then one would need new material such as that now being integrated into police departments, the recruiting of personnel able to handle tomorrow's police tasks and a training that will ensure the optimal use of the instruments to be used by the police officers. Training, necessarily, will become specialized and high level in order that

trainees may understand the operational side of the technology and meet community needs. This is something that the French government noted during the national training conference which took place in February 1999 in Paris (France, 1999).

MIS technicians and systems specialists will be required within the police force. A small police department like the one at Hull, in Quebec, which has a payroll of about 100 police officers, hired a computer technician five years ago as a full time employee. He manages the networks, plans out changes to current technology, reboots the system when it goes down, designs new computerized applications and looks after the management of the area. He also ensures that the systems meet maximum security criteria in order to protect the police information service. And he tries to ensure that the systems selected by the department are compatible with those of other police departments.

Ethics and Liability

There can be no area where it is more necessary to scrutinize the ethical side of police activities than when it comes to using technology. Indeed, it is true that for a considerable time now we have accepted that a computerized system such as the Canadian Police Information Centre (CPIC) must be protected because it contains a great deal of information on individuals. This also means, given the ease of interconnection and the speed of existing software, that it is essential to ensure that police accessing this type of data bank, to input and extract information. should use it exclusively within the framework of their mandate (Marx, 1998). A commission of inquiry recently revealed that police officers had used data obtained from a data bank for personal ends (Sûreté du Québec Public Inquiry Commission, 1998). Something that is unacceptable but exceptional may turn into an everyday habit if an ethical reflexion on technology and its use is not begun and pursued. Technology must not be used for purposes for which it was not designed. We should remind those concerned that ethics should be part of the daily life of all police officers, whatever their rank, function or the extent of their personal ambitions within the police force. The ethical approach which is first presented in the classroom should be maintained and encouraged in the police officer's daily activities. It would also be salutary if unethical behaviour were reported, but this seems still a lot to hope for in the light of contemporary police culture.

Another issue is that of the liability of police departments when they use technology and the legal proceedings that may ensue. The use of non-lethal weapons such as cayenne pepper (oleoresin capsicum), which is permitted because it constitutes an alternative to regular weaponry, has led to court proceedings in the United States which resulted in the conviction of police officers who used pepper sprays against a rambunctious offender (Cansler, 1998). Again, intercepting private communications when access is prohibited by the use of keys raises the question of the right to privacy and the right to the protection of the public at large (Cansler, 1996). However, one thing is certain: technology should not be improperly used or used for purposes for which it was not intended.

One may also suppose that the new work methods based on high-tech apparatus will allow police officers to take suspects' statements at the scene of the crime or in the patrol car, a practice that is current in the London (Ontario) police department. There, thanks to a PC which stocks the requisite forms, the suspect confirms the accuracy of his statement, not by signing it, but by clicking on the 'Send' button, which immediately transmits the statement to the H.Q. data bank. Another problem is that mug-shot files, which offer an extended choice of suspects for crime, could be a source of difficulty for crime control. Digital photos can be modified by computer without there being any trace of a change. In other words, a photograph could be modified to suit the characteristics of a suspect so that they look alike. This rather silly example allows us to stress the fact that police work is being simplified and refined thanks to the technology, but we still have to see how the law will deal with the introduction of these new techniques.

Finally, there is the major question of encrypting, which raises a number of basic questions. Encrypting is the ability to hide the content of the message by making it incomprehensible except to authorized recipients. We know that Internet was financed by the US Army during the cold war in order to increase the number of communication sources in the event of a major nuclear attack. Internet is a huge worldwide computer network, and in 1997 it was estimated that it included some 80,000 independent computer networks (Dobeck, 1997). This means that it is fairly difficult for law enforcement services to penetrate the

system. One of the solutions proposed by the United States is that government should have control over servers, a suggestion which has not been unanimously welcomed and which runs counter to the very principle of Internet and of the right to privacy (Pilant, 1999).

Concluding Remarks

A great number of the factors affecting the role of technology in the police depend to a large extent on social forces whose interaction and development are not easy to predict. The future of technology is based on strictly human considerations: a police chief who is motivated by technology, specialists who work to get a file accepted, budgets that are developed under pressure from seasoned warriors in the field. Technology is there to hand, but it is up to the decision-makers to understand this.

There are already studies on the way in which police departments collate and analyse data (types, objectives, etc.) and also how the police access such data (O'Shea, 1998). There are others in which the emphasis is on the extent to which technology diminishes the number of reports and forms that have to be drafted or filled in (Moriarty, Dover, 1998). There are yet again others based on surveys of target groups that indicate that computer crimes (copying or illegally selling software, illegal intrusion by hackers) are not necessarily seen as crimes, and particularly not by students in engineering or technology (Mercier, 1998).

If, as we have noted, the introduction of technological tools requires planning in terms of costs and modification of functions, it is still true that the development of these tools is being pursued at an extraordinary rate, as is their marketing. On one hand, police officers ask their superiors to provide apparatus to facilitate and improve the carrying out of their tasks; on the other hand, management is under pressure from the market itself, which sweet-talks them about the advantages and benefits of highly developed tools, advantages that sometimes go well beyond the real needs of the departments, or create new setting-up costs because the systems are incompatible.

There is, indeed, no rational approach to integration or use of technology. We suspect that the decision-making in this area is based on a transient rationalization supported by knowledge and skills that are external to and uncontrollable by the police itself. The lack of familiarity with the tools means that they are integrated only partially or superficially, in an attempt to make them compatible with traditional work methods. In the end, technology necessarily goes through a transitional phase where the police have to first learn to come to terms with tools that promise effective problem solving before they can integrate them and use them properly. It is essential that we do not become too independent of our suppliers and of those who control the market (Naulleau, 1998). Once the transitional phase has been completed, a phase that can be quite long, given the human and financial factors involved, it is still necessary to learn how to integrate these new tools with the classic working methods with which the police are familiar and which were developed much earlier. Since it is necessary that users be trained to adapt to the tools, and that experts be on-site or reasonably available to help or to handle the apparatus, which means reorganizing human resources, integration is like a game of leap-frog—up and over, down and across.

Not only must we prepare police departments to understand the major changes that will be caused by the introduction of high-performance technological tools, tools that are completely new within the field of police work, we must also prepare them to integrate these tools, to handle them properly, so that they do not lag behind when it comes to dealing either with new forms of crime that derive from such technology, or with more traditional criminal behaviour. It may be fairly easy to understand that computer fraud requires up-to-date skills and specialized knowledge, but one must also realize that crime control is also dependent on new tools such as remote detection (Quirion, Lamy, 1999), and that these techniques have to be learned by active police officers.

References

Akrich, M.; Méadel, C. (1993). Technologies de sécurité et organisation. *Les Cahiers de la sécurité intérieure,*21:53-59.

Anderson, P. B. (1997). Web Technology in Law Enforcement. Page web consultée le 1999-4-26.

Audet, M.; Jacob, R.; Lauzon, N.; Rondeau, A. (1996). *Renouvellement des services publics et autoroute de l'information: vers un modèle stratégique de transformation et de critères d'aide à la décision.* Version finale. Présenté au Centre francophone de recherche en informatisation des organisations (CEFRIO). Septembre.

Boullier, D. (1993). La vidéosurveillance à la RATP: un maillon controversé de la chaîne de production de sécurité. *Les Cahiers de la sécurité intérieure,* 21:88-100.

Brady, T. (1996). The Evolution of Police Technology. In National Institute of Justice, Office of Community Oriented Policing Services (ed) *Technology for Community Policing.* Conference Report. National Institute of Justice.

Bratton, W.; Nobler, P. (1998). Turn Around. How America's Top Cop Reversed the Crime Epidemic. New York: Random House.

Breton, P. (1966). L'informaticien et la sécurité: enquête sur un antagonisme. *Les Cahiers de la sécurité intérieure,* Entreprise et sécurité, 24:36-47.

Bulletin sur la sécurité de l'informatique. (1998). Sous-direction de la sécurité des technologies de l'information, GRC. Sécurité des TI. Janvier. No 45.

Campbell, F. (1997). High-Tech Advances Bring New Tools. *Police*, 21, 10:60-63.

Cansler, R. (1996). Technology Liability Considerations. In National Institute of Justice, Office of Community Oriented Policing Services (ed) *Technology for Community Policing.* Conference Report. National Institute of Justice.

Cansler, R.E. (1998). Technology Liability Considerations. *The police Chief*, May:53-55.

Carpenter, G. (1984). Preliminary Considerations for the Impact of Microtechnology on Police Management. *Canadian Police College Journal*, 8, 2:93-106.

Carter, D.; Katz, A. (998). Computer Applications by International Organized Crime Groups. In L. Moriarty; D. Carter (eds.) *Criminal Justice Technology in the 21st Century.* Springfield: Charles C. Thomas.

Castells, M. (1996). *The Rise of the Network Society.* The Information Age: Economy, Society and Culture. Volume I. Great Britain; Blackwell.

Catalyst (1996). Denver Partnerships Produce Unexpected Evidence, 16, 2:1-2.

Clarke, R. (1993). Les technologies de la prévention situationnelle. *Les Cahiers de la sécurité intérieure*, 21:101-112.

Corsentino, D.; Pettinari, D. (1996). A Fork in the Road. *Sheriff*, March-April:1012, 35.

Coutorie, L. E. (1995). The Future of High-Technology Crime: A Parallel Delphi Study. *Journal of Criminal Justice*, 233, 1:13-27.

Dobeck, M. (1997). Taking Advantage of the Internet. *The Police Chief*, January:35-38.

Dorn, N. (1998). Du renseignement au partage des informations: l'intelligence protéiforme. *Les Cahiers de la sécurité intérieure*, 34:91-108.

Ericson, R.; Haggerty, K. (1997). *Policing the Risk Society*. Toronto: University of Toronto Press.

France, Ministère de l'Intérieur (1999). Assises de la formation et de la recherche dans la police nationale

(1999). Table ronde no 2: former à l'utilisation des technologies nouvelles. Paris: La Villette.

Fulton, R. (1995). When Law Enforcement Met Industry, Transferring Military Technology. *Law Enforcement Technology*, September:56-60.

Galland, J.P. (1996). Eléments pour une prospective de la sécurité. *Les cahiers de la sécurité intérieure*, 24, Deuxième trimestre:85-102.

Goodman, M.D. (1997). Working the Net. Exploiting Technology to Increase Community Involvement and Enhance Service Delivery. *The Police Chief*, August:45-53.

Grabosky, P. ; Smith, R.; Wright, P. (1996). Crime and Telecommunications. Trends and Issues. *Crime and Criminal Justice*, 59: .

Green Mazerolle, L.; Haas, R. (1998). 'The problem Solver'. The Development of Information Technology to Support Problem-Oriented Policing. In L. Moriarty; D. Carter (eds.) *Criminal Justice Technology in the 21st Century*. Springfield: Charles C. Thomas.

Haley, K.; Taylor, R. (1998). Police Stations in Cyberspace: A Content Analysis of Law Enforcement Agency Home Pages. In L. Moriarty; D. Carter (eds.) *Criminal Justice Technology in the 21st Century*. Springfield: Charles C. Thomas.

Hutchison, J.; Mays, J.; Moriarty, L. (1998). Teaching Statistics in the 21st Century: Technology in the Classroom. In L. Moriarty; D. Carter (eds.) *Criminal Justice Technology in the 21st Century*. Springfield: Charles C. Thomas.

Johnson, R. (1997). High-Tech Help. Robots Lend a Hand in the Labs. *Pony Express*, December: 18-19.

Kerr, J. (1999a). Inside the Web. Intranet Pilot Project Keeps the Force Connected. *Pony Express*, January-February: 7.

Kerr, J. (1999b). Making Connections, Computer Database Helps Investigators Piece Organized Crime Networks Together. *Pony Express*, January-February:16.

LeBeuf, M.E. (1998). Redefining Police-Community Relationships. Ottawa: Research Centre. Canadian Police College.

LeBeuf, M. E. (1999). Police de proximité et contrats locaux de sécurité- Que retenir du modèle canadien de police communautaire? Rapport présenté à l'Institut des Hautes Etudes de la Securité Intérieure-IHESI. Janvier.

Lingerfelt, J. (1996). Technology as a Force Multiplier. In National Institute of Justice, Office of Community Oriented Policing Services (ed) *Technology for Community Policing*. Conference Report. National Institute of Justice.

Loree, D. (1987). Technological Innovation and Social Control: Some Implications for Police. *Canadian Police College Journal*, 11, 1:13-33.

MacDonald, V.; Martin, M.(1986). Specialists and the Personnel Structures of Canadian Police Forces. *Canadian Police College Journal*, 10, 3:189-226.

Manning, P. (1992). Technological and Material Resource Issues. In L. T. Hoover (ed.) *Police Management Issues & Perspectives*.

Martin, S. (1996). *The Impact of Information Technology Upon the Traditional Hierarchical Structures in Highly Bureaucratic Organizations*. Command College Class XXI. Peace Officer Standards and Training. Sacramento, California.

Marx, G. (1997). The Declining Significance of Traditional Borders (and the Appearance of New Borders) in an Age of High Technology. In P. Drogue (ed.) *Intelligent Environments*. Elsevier Science.

Marx, G. (1998). An Ethics For The New Surveillance. Page web consultée le 1998-10-2.

McLean-Lipinski, J.R. (1999). Enhancing the Use of Tehcnology in Law Enforcement. Page web consultée le 1999-05-06.

Mercier, P. (1998). On-Line Crime: In Pursuit of Cyber Thieves. In L. Moriarty; D. Carter (eds.) *Criminal Justice Technology in the 21st Century*. Springfield: Charles C. Thomas.

Moore, R.H. (1995). Technology and Private Security; What Does the Future Hold? Journal of Security Administration,.18,2:1-9.

Moriarty, L.; Dover, T. (1998). The Centralized Data Entry (CDE) System: One County's Attempt at Managing Burdensome Paperwork with Innovative Technology. In L. Moriarty; D. Carter (eds.) *Criminal Justice Technology in the 21st Century*. Springfield: Charles C. Thomas.

Morrison, R. (1996). Information Technology 2000. What's Ahead in the 21st Century. *Law Enforcement Technology*, June:40-43.

Myers, L.; Myers, L. (1998). Integrating Computers in the Classroom: A National Survey of Criminal Jusitice Educators. In L. Moriarty; D. Carter (eds.) *Criminal Justice Technology in the 21st Century*. Springfield: Charles C. Thomas.

National Institute of Justice (1994). *25 Years of Criminal Justice Research*. National Institute of Justice. December.

National Institute of Justice (1997). *Technology for Community Policing*. Conference Report. Sponsored by National Institute of Justice, Office of Community Oriented Policing Services, National Institute of Justice. June.

Naulleau, D. (1998). Le bogue de l'an 2000: un révélateur de la vulnérabilité de nos libertés. *Les Cahiers de la sécurité intérieure*, 34:69-90.

Nogala, D. (1993). Le rôle de la technologie dans la police de demain. *Les cahiers de la sécurité intérieure*, 14, août-octobre:137-158.

O'Shea, T. (1998). Analyzing Police Department Data: How and How Well Police Officers and POlice Departments Manage the Data They Collect. In L. Moriarty; D. Carter (eds.) *Criminal Justice Technology in the 21st Century*. Springfield: Charles C. Thomas.

Ocqueteau, F.; Pottier, M.L. (1993). Vidéosurveillance et gestion de l'insécurité dans un centre commercial: les leçons de l'observation. *Les Cahiers de la sécurité intérieure, 21:60-74*.

Parsons, S. L. (1993). Technology Can Boost Safety in the Field. *Police and Security News*, 9,4:19-22,27.

Pilant, L. (1999) The Debate Over Encryption. *The Police Chief*, LXVI, 1:31-35.

Pilant, L. (1994). Spotlight on High-Tech Training. *The Police Chief*, July: 25, 27-33.

Pitcher, P. (1995). *Artist, Crafstmen and Technocrats: the Dreams, Realities and Illusions of Leadership*. Toronto: Stoddart.

Preimsberger, D. (1996). Cops and Space Scientist:New Crime-Fighting Partners. *The Police Chief*, October:108-114.

Public Inquiry Commission Appointed to Inquire into the Surete du Quebec (1999). Report of the Public Inquiry Commission Appointed to Inquire into the Surete du Quebec. Vol. 1, 2. Summary and Recommendations. Québec: Les Publications du Québec.

Quirion, S.; Lamy, O. (1999) La télédétection appliquée aux cultures agricoles et illicites. Sommets, 13, 2:22.

Rodriguez, M. (1995). An Overview of Law Enforcement Technology. *The Police Chief*, April: 15-29.

Rosé, P. (1996). L'informaticien et la sécurité de l'entreprise. *Les cahiers de la sécurité intérieure*, 24: 25-35.

Seaskaste, Inc. (1998). *The Evolution and Development of Police Technology*. A technical Report prepared for The National Committee on Criminal Justice Technology. National Institute of Justice.

Sheptycki, J. (1998). Reflections on the Transnationalization of Policing; the Case of the RCMP and Serial

Killers. *International Journal of the Sociology of Law*, 26:17-34.

Sloan, R.C. (1997). How Can Technology Help Police Be More Effective in Community Policing? In National Institute of Justice, Office of Community Oriented Policing Services (ed) *Technology for Community Policing*. Conference Report. National Institute of Justice.

Smietan, I.; Ferris, D. (1996). Detecting Concealed Weapons. In National Institute of Justice, Office of Community Oriented Policing Services (ed) *Technology for Community Policing*. Conference Report. National Institute of Justice.

Soullière, N. (1999). Police et technologies: un bilan historique, un regard contemporain. Ottawa: Collège canadien de police, Centre de recherche.

Strandberg, K. (1998). Websites For Law Enforcement. *Law Enforcement Technology*, January:59-60.

Tafoya, W. (1997). Policing High Tech Crime. *Crime & Justice*, October, 23.

Wells, J.; Minor, K. (1998). Criminal Justice Students' Attitudes Toward Distance Learning as a Function of Demographics. In L. Moriarty; D. Carter (eds.) *Criminal Justice Technology in the 21st Century*. Springfield: Charles C. Thomas.

Wilsker, I. (1997). Cops on the Web. In National Institute of Justice, Office of Community Oriented Policing Services (ed) *Technology for Community Policing*. Conference Report. National Institute of Justice.

La police et l'usage des technologies de l'information: un bilan actuel

par

Marcel-Eugène LeBeuf, Ph.D.

Centre de recherche

Collège canadien de police

Ottawa, 1999

Introduction

La police se confronte présentement à un nouveau paradigme. Elle passe lentement d'une période où pendant longtemps elle a contrôlé totalement son champ d'intervention à une période, qui n'en est pas une de transition, où arrivent simultanément une criminalité technologique qui ne possède aucun des caractères du crime traditionnel, de nouveaux outils d'intervention performants mais nécessitant une formation spécialisée de haut niveau, et une expression plus forte des citoyens par rapport à ce qu'ils veulent que leur police accomplisse dans leurs lieux de vie.

Ce document expose sommairement différents enjeux relatifs à l'implantation et à l'usage des technologies de l'information dans la sécurité publique. Il tient compte aussi de l'arrivée d'une nouvelle criminalité impliquant les technologies et qui n'a aucun rapport avec la criminalité traditionnelle connue. Il examine des pistes de solutions qui pourront aider les agences de mise en application de la loi à se préparer aux technologies, ce qu'elles ont à peine commencé à faire (Tafoya, 1995).

L'expression de technologie de l'information est ambiguë, générale et porte en elle-même les limites de sa compréhension. Elle désigne une variété de gadgets, de machines, de logiciels plus ou moins complexes et qui, dans les termes de Nogala (1993), ont une logique d'évolution, un emploi et un impact qui leur est propre. Toutefois cette expression amène deux questions essentielles, simples à formuler mais difficiles à répondre: quelles sont les technologies de l'information utiles à la police? Comment l'intégration des technologies modifie-t-elle le rôle et les tâches de la police?

Ce document situe l'avance des technologies de l'information dans le domaine de la sécurité publique. Sans prétendre être exhaustif, nous nous pencherons sur plusieurs aspects clés des technologies sans ordre d'importance:

- les technologies de l'information et la police
- l'intégration des technologies au monde traditionnel de la police
- l'informatisation de la police?
- les usagers des technologies dans un service de police
- la mise en place des outils technologiques
- les facteurs incitatifs et de blocage
- les coûts des technologies
- l'impact des technologies sur le fonctionnement de la police
- la formation pour les technologies de l'information
- l'éthique et les responsabilités professionnelles

Les technologies de l'information et la police

Les relations entre la police et les technologies sont complexes et non linéaires. Elles touchent à la fois au pouvoir et à l'information. De façon schématique on dira que les technologies de l'information favorisent des actions et l'obtention de résultats qui étaient impossibles à atteindre auparavant. Par là, le fonctionnement de la police est amélioré (Manning, 1992). De plus, son image dans le public et son impact dans la société s'améliorent nettement. A cet effet, les pages *web* des services de police constituent un excellent exemple. Elles sont des entreprises novatrices de relations publiques pour informer la population des expériences de prévention du crime menées dans leur milieu, ou de l'état de la criminalité ou encore un support d'information pour les personnes disparues (Strandberg, 1998; Haley, Taylor, 1998; Goodman, 1997; Wilsker, 1997; Anderson, 1997; Corsentino, Pettinari, 1996).

Par ailleurs grâce aux renseignements colligées par la police, il n'est pas faux de dire que les technologies de l'information permettent de maintenir son pouvoir symbolique dans les communautés (Ericson, Haggerty, 1997). En effet, il ressort que l'accès aux banques de données et aux autres outils informatiques donne plus de renseignements et permet conséquemment de développer des stratégies plus efficaces pour lutter contre les crimes traditionnels mais aussi contre les crimes reliés à l'usage des technologies (high tech crime) (McLean-Lipinski, 1999). Comme le travail de police est écologiquement dispersé dans les termes de Manning (1992), l'efficacité prétendue dépend de plusieurs facteurs dont la

culture organisationnelle des différents groupes de travailleurs, le type de renseignements retenus et les méthodes pour le faire. La guerre des informations (information warfare) constitue une menace réelle illustrée par le blanchiment d'argent, les jeux de hasard, les extorsions de toutes sortes dont les cartes de crédit ou la falsification de données par un ordinateur, les crimes économiques, l'attaque de systèmes informatiques, le piratage électronique, l'espionnage et d'autres activités des groupes reliés au crime organisé (Coutorie, 1995; Dobeck, 1997; Carter, Katz, 1998). Pour ces crimes, il n'est plus nécessaire de se déplacer physiquement. Un nouvel univers virtuel désormais en place y pallie et devient le véritable enjeu (Rosé, 1996). Les nouvelles connections sont horizontales et invisibles (Marx, 1997). Le gagnant est celui qui contrôlera les rênes de cet univers. Si les organes d'application de la loi veulent être aussi rusés (smart) que les criminels, ils doivent adopter les outils technologiques qui se trouvent sur le marché (Campbell, 1997). Le défi à relever est moins d'adopter les technologies de l'information que qu'adapter celles qui amélioreront réellement les habiletés à contrecarrer systématiquement les problèmes posés à la police.

L'intégration des technologies au monde traditionnel de la police

Il est relativement difficile de tracer un bilan actuel de l'usage que fait la police des technologies. Les technologies font partie du monde policier depuis plus de 150 ans (Soullière, 1999). Or, jusqu'à présent, il ressort que prises dans leur ensemble elles apparaissent ponctuellement et de façon erratique dans divers services de police à travers le Canada. Il y a plus de 15 ans que leur utilité a été constatée (Carpenter, 1984). Par ailleurs, le marché privé des technologies se développe à un rythme extrêmement rapide et qui est inversement proportionnel à celui de la prise de décision dans les services de police publics. C'est dire que la police représente un marché à exploiter et qu'il faut le faire rapidement. C'est dire aussi que la police doit apprendre à définir ses besoins internes et les besoins de la communauté qu'elle dessert pour parvenir à faire une sélection éclairée des outils les plus appropriés.

Il est connu que dans la police des preneurs de décision ne possèdent pas toujours les habiletés pour prendre les décisions qui s'imposent (Carpenter, 1984) ou encore pour s'engager dans un processus de prise de décision (MacDonald, Martin, 1986) relatif à un processus dont les ramifications sont depuis un bon moment difficiles à déterminer (Loree, 1987). Confrontés aux technologies, la situation devient encore plus difficile dans le sens où le décideur fait face à des outils nouveaux, performants si bien utilisés, et en même temps, presque totalement étrangers à l'univers policier traditionnel (Martin, 1996).

Dans beaucoup de cas, plusieurs éléments sont nouveaux: la technologie comme telle (système AFIS-identification des empreintes digitales automatiques), le rapport au travail traditionnel, et la capacité d exploiter complètement la technologie. Au cours d'une visite, une policière nous a fait la démonstration du système géocrime ou plus connu sous le nom de *crime mapping*. Lors de manipulations, la policière confiait qu'il lui avait fallu plus de huit mois pour apprendre à manipuler le logiciel qui, à l'évidence, pouvait produire des résultats bien supérieurs à ceux auxquels elle parvenait faute de *coaching* mais aussi d'expertise dans la gestion des données et de l'outil.

Cet exemple montre que les outils technologiques sont performants, surtout s'ils ont été développés pour la police ou encore avec celle-ci. Il semble que la performance est toute relative dans le sens où l'usage d'un logiciel, par exemple, donne un supplément d'information dans la mesure où l'usager sait utiliser complètement son potentiel. Qui de nous, faisant usage de logiciels de traitement de texte comme le *Word Perfect* ou *Word* ne se rappelle pas avoir découvert des subtilités dans leurs applications après plusieurs années d'usage au quotidien? La performance d'un appareil ne doit pas occulter que son utilisateur crée des limites par le rapport qu'il entretient avec celui-ci. Il ne doit pas non plus faire oublier aux décideurs que chaque logiciel crée ses propres contraintes quand il est intégré dans un ensemble technologique vaste.

Pourquoi informatiser la police?

Les nouvelles technologies favorisent le renouvellement de la prestation des services afin de répondre

aux besoins des utilisateurs payeurs, la population (Audet et al.,1996). Elles facilitent une démarche vers un virage vers une police de service aux citoyens, une police communautaire comme on pourrait le dire. La population réclame des services publics plus performants à la lumière des fonds qui leur sont consacrés (LeBeuf, 1998). A cela s'ajoute la nécessité de répondre aux besoins des usagers - les policiers - dans un contexte de changement de paradigme d'une police traditionnelle réactive vers une police plus proactive. A cet effet, le Service des relations communautaires de la Sûreté du Québec a développé un outil de référence- le projet ARC (activités en relations communautaires) qui comptabilise toutes les interventions accomplies par les policiers dans le cadre de la prévention du crime.

Pour répondre aux clients, les organisations mettent en place des structures intelligentes qui permettent d'intervenir rapidement, localement, avec compétence et autonomie décisionnelle. De nos jours, plusieurs services de police ont intégré certains des outils technologiques pour l'identification judiciaire comme le *AFIS* (automated fingerprint identification system*)* pour les empreintes digitales, ou pour les communications le GPS (global positioning system), ou encore l'ordinateur véhiculaire. Il reste à tracer un bilan plus élaboré de la situation des polices au pays. Par ailleurs, il faut ajouter aussi qu'à l'interne le rapport entre les patrons et les employés se transforme grâce à l'autonomie donnée et vécue par les employés qui ont des accès plus directs à des banques de données, et conséquemment, aux stratégies à actualiser.

Par ailleurs, le marché de la sécurité privée étant novateur et préoccupé avant tout par la protection des biens, les outils développés et utilisés sont souvent à l'avant-garde de ce que se permet la sécurité publique. Ce n'est qu'une question de temps, non de décennies, pour que des grands domaines de la protection, des lieux, des biens et des personnes ne soient plus assurés par l'intervention humaine mais par la robotique, l'usage de satellites, la nanotechnologie, la micro-*engineering (*Moore,1995; Akrich, Méadel, 1993). Moore (1995:2) donne l'exemple de périmètres de sécurité qui pourront être désormais établis par des rayons lumineux invisibles mais sensibles au mouvement, ou encore par le laser, ou le *pulsar.* De même, la robotique a un usage exceptionnel dans les laboratoires grâces aux manipulations sensibles qu'elle rend possible lors d'extractions de composés chimiques par exemple (Johnson, 1997). La technologie de la biométrie qui rassemble les empreintes digitales, les empreintes des paumes de la main, les traits spécifiques du visage, la lecture de la rétine ou de l'iris, deviendra le système d'identification du futur. Dans le même ordre d'idées l'identification par l'A.D.N. (Acide désoxyribonucléique) est appelée à devenir une forme d'identification commune. A cet effet, rappelons que le parlement canadien a adopté la Loi sur l'identification par les empreintes génétiques qui permet de créer un banque donnée de l'A.D.N. de personnes condamnées pour des infractions graves.

Les usagers des technologies dans un service de police

Les usagers des technologies dans un service de police sont aussi différents qu'il y a de tâches à accomplir. Selon l'outil dont on parle, comme le géocrime ou l'ordinateur véhiculaire, les usagers ne sont pas les mêmes. Dans le premier cas, les analystes disposant d'un tel logiciel ont la tâche d'aller chercher le plus de renseignements possibles dans différentes banques de données afin d' éclairer par la suite les enquêteurs et ultimement les patrouilleurs. Toutefois, ni les enquêteurs ni les patrouilleurs n'ont un accès direct ou un accès limité aux mêmes banques de données. Dans le cas des ordinateurs véhiculaires, les patrouilleurs traitent les renseignements directement dans leur véhicule de patrouille. Ils accèdent à du matériel qui leur permet d'améliorer leur tâche et souvent de la simplifier, en éliminant souvent les nombreux formulaires à compléter. Le Service de police de London en Ontario a simplifié les procédures en offrant aux patrouilleurs l'accès aux formulaires à partir de leur véhicule de patrouille.

Plus globalement et pour simplifier notre démonstration, on pourrait catégoriser les usagers en quatre grands types: le gestionnaire, l'enquêteur, le patrouilleur et les partenaires. Il faut se rappeler que toute forme de catégorisation élimine nécessairement la complexité d'une démonstration.

Le gestionnaire de haut niveau ou le responsable d'une équipe fait face à une diminution des ressource financières et humaines. Il sera appelé à développer le réflexe de recourir aux avancements dans le domaine des technologies pour que les tâches soient accomplies autrement (Morrison, 1996). Or, plus souvent qu'autrement le gestionnaire a été formé et travaille avec des méthodes d'un environnement pré-

technologique (Rodriguez, 1995). Il lui appartient de développer ses besoins au plan de sa compréhension des outils technologiques, d'une vision de la technologie qui corresponde à la vision stratégique et corporative de son organisation, de créer des structures organisationnelles flexibles pour gérer le travail et les individus, d'encourager la coopération latérale entre les unités, et surtout de posséder et de contrôler un processus de prise de décision basé sur les compétences et non sur le rang (Martin, 1996).

Par ailleurs, l'enquêteur d'unités du crime organisé ou de la criminalité informatique par exemple est soumis à appréhender de nouveaux outils pour affronter les défis posés par ces formes de criminalité. Désormais, l'enquêteur muni de son mandat de perquisition saisit moins les livres ou autres documents d'un autre âge que des ordinateurs portatifs, des disques durs. Il intercepte des communications faites par téléphones cellulaires codés, etc. En d'autres mots, il est confronté à l'univers de la technologie des communications qui touche la société en général, mais qui est aussi utilisé pour des actions contrevenant à la loi.

L'analyste de la criminalité de son côté est confronté à une quantité phénoménale de banques de données qui offrent du matériel pertinent au travail. Comment alors parvenir à faire la bonne sélection du matériel à la lumière des besoins à combler? Une des premières conséquences de l'accès à du matériel aussi nombreux est que l'analyste doit apprendre à penser différemment. Plutôt que de se concentrer sur un seul problème, il doit développer le réflexe d'approcher plusieurs problèmes et plusieurs pistes de solution à la fois. Quelques fois il le fera aussi avec des collègues dispersés géographiquement et possédant une expérience et des langages différents (Dorn, 1998). L'analyste, comme d'autres, se retrouve confronté au trop de savoir. Les données demeurent insignifiantes à moins qu'elles ne soient transformées dans un langage significatif aux plans des opérations et/ou de la gestion. Les nouveaux outils modifient nécessairement les façons de voir et d'analyser les crimes. Le VICLAS (violent crime linkage analysis system) par exemple, utilisé pour élucider les meurtres en série, transforme l'approche que les enquêteurs ont avec les données qu'ils accumulent (Sheptycki,1998). L'usage des technologies à outrance risque-t-il de devenir inutile pour la police par les difficultés du traitement?

Le patrouilleur, selon le service de police, se retrouve dans des véhicules de patrouille qui sont devenus de véritables laboratoires informatiques ambulants. Si d'une part, un certain nombre de tâches ennuyantes et répétitives peuvent être diminuées grâce à des banques de données et à des logiciels qui donnent des formulaires simplifiés, il reste que le patrouilleur doit aussi apprendre à gérer et à coordonner les outils qu'on lui fournit allant de la caméra qui le filme lorsqu'il sort de son véhicule, à l'ordinateur véhiculaire et/ou portatif, ou encore à l'ordinateur de bord, au courrier électronique, à et bien d'autres encore. Ces outils améliorent la sécurité des policiers et leur performance (Parsons, 1993). Constatons que le patrouilleur de demain sera peut être communautaire (LeBeuf, 1999), cela reste à voir, mais il sera certainement technologique.

Par ailleurs, comme les technologies de l'information éliminent en général un certain nombre de tâches dans une fonction, on serait porté à penser qu'il se développerait une collégialité et une collaboration entre les collègues et avec les spécialistes de l'informatique dans les services de police. D'ailleurs, à cet effet, ne rappelle-t-on pas de sortir ces spécialistes de leur bureau et de les inciter à collaborer avec les policiers pour adapter les technologies à leurs besoins. L'ingénieur responsable du développement des systèmes informatiques du Service de police de la Communauté urbaine de Montréal a insisté pour intégrer des policiers de première ligne à sa structure de travail pour élaborer des systèmes qui rencontrent leurs besoins.

Or, contrairement à ce que l'on pourrait penser, les technologies confinent davantage les individus dans des tâches qui nécessitent une grande compétence. Elles conduisent à développer une expertise pointue. Une fois qu'un analyste a appris à manipuler les logiciels du géocrime par exemple, il finit par découvrir le potentiel de l'outil. En d'autres mots, l'individu finit par devenir performant moins comme policier que comme expert dans la gestion d'un logiciel pour une tâche donnée. Il a appris par la nouvelle structuration des méthodes de travail à comprendre et à définir la réalité du crime dans toute sa complexité, éliminant par là les facteurs explicatifs simplistes (Catalyst, 1996). Muter cet individu à l'intérieur du service signifie qu'il y aura de nouveaux coûts de formation mais surtout qu'il y aura nécessairement une période de flottement où l'analyse de la criminalité ne pourra pas être accomplie avec le même niveau de compétence qu'auparavant.

Enfin, une autre catégorie d'usagers qui se situe dans un rapport très particulier avec les technologies concerne les partenariats possibles entre la police et l'industrie ou encore entre la police et des gouvernements. Diverses expériences de partenariat américaines commentées montrent comment la police gagne à collaborer avec la grande industrie privée (Fulton, 1995), ou encore avec des services du gouvernement comme l'armée (Smietan, Ferris, 1996; Preimsberger, 1996). La réflexion sur les armes non vulnérantes (non lethal) a conduit à des considérations majeures au plan des interventions policières telles: le *smart gun* ou le *stricky foam* (un spray qui immobilise un sujet dangereux, le *road patriot* (qui arrête un véhicule en déconnectant son système électrique), l'imagerie du miroir (Imagery process mirrors) développée par les chercheurs de l'espace pour améliorer substantiellement des images floues ou incorrectes), le *GPS* fournit la latitude et la longitude des patrouilleurs et permet de les retracer rapidement. Le Service de police de la MRC des Collines-de-l'Outaouais qui couvre un grand territoire rural peut, par cet outil technologique, assurer une plus grande sécurité à son personnel et une réponse plus rapide aux citoyens.

Une autre forme de partenariat résulte des possibilités d'échanges de renseignements entre la police et des organismes communautaires par le biais de systèmes d'information plus performants (Catalyst, 1996). Il ressort par là que la police n'est plus l'unique dépositaire de ce qui se passe dans la collectivité, mais surtout que des échanges constructifs sont facilement concevables par les technologies. La question demeure: comment faire pour que l'usage des technologies améliore les habiletés pour diagnostiquer systématiquement les problèmes sociaux (Sloan, 1996)?

Il faut s'empêcher de faire des généralisations hâtives au moment où la police est encore souvent à l'essai et à l'erreur dans l'apprentissage de nouveaux outils qui encore dernièrement, étaient étrangers aux policiers et aux méthodes de formation pour la tâche.

La mise en place des outils technologiques

Au début des années 90, un service de police de grande taille au Canada décidait d'intégrer la technologie récente en identité judiciaire. Le processus qui a duré cinq années, a structuré le système *AFIS* et élimine un grand nombre de formulaires et de documents en filières. L'ère du *paperless* est commencée. Or, ces cinq années de changement majeur se sont révélées turbulentes à plusieurs points de vue. En effet, s'il est vrai qu'une planification sur papier avait été développée, un certain nombre de problèmes lourds sont apparus en cours du processus de changement: des fournisseurs ont fait faillite; certaines bases de données ne pouvaient pas être connectées parce que les plates formes n'étaient pas compatibles; lors des transferts des données manuelles contenues dans des filières à des banques de données informatisées, il est arrivé à plusieurs reprises que les systèmes tombent en panne, ce qui a provoqué des critiques acerbes; enfin, la destruction des vieux dossiers a entraîné des réactions extrêmement violentes de la part des employés qui voyaient leurs notes manuscrites mises aux poubelles. Une fois le processus complété, le système nécessite deux postes de travail comparés aux 28 postes précédents.

Une des difficultés majeures qui confronte le gestionnaire est de parvenir à développer un plan stratégique pour rencontrer les processus au quotidien. La meilleure planification d'un changement ne peut donner de bons résultats que dans la mesure où elle tient compte à la fois de l'évolution des outils, des mentalités et des facteurs de résistance au changement. Les technologies sont manipulées par des hommes et des femmes soumis à divers stress reliés à la tâche policière, mais aussi au cadre professionnel. L'un et l'autre affectent autant les résultats souhaités par l'implantation des technologies.

Par ailleurs, la mise en place de systèmes informatiques nécessite aussi une capacité d'accueil pour des experts qui assurent le fonctionnement à court et à moyen terme. Il est fascinant de remarquer que des services de police se sont adjoints des experts de compagnies informatiques ou encore ont créé des postes de membres civils, ingénieurs en informatique, informaticiens, etc, pour assurer l'intendance des systèmes, leur planification et les stratégies de remplacement. Le nouveau créateur (Pitcher, 1995) dans la police se nomme informaticien ou gérant des technologies. La police voit donc l'arrivée de ces spécialistes hautement qualifiés moins pour gérer des domaines scientifiques comme les laboratoires que pour planifier et élaborer des programmes informatiques experts pour l'ensemble des membres (comme les terminaux véhiculaires) (Breton, 1996).

Il arrive que le produit offert par les compagnies ne réponde pas bien aux demandes de la police. Alors, il convient de développer avec la compagnie un produit qui rencontrera les besoins de la police. Comme on nous le mentionnait, "si le produit n'existe pas, on le fait créer mais cela demande une énorme implication". Or, ce n'est pas le rôle de la police mais celui des chercheurs qui, sensibilisés à la complexité de la tâche policière, créent de nouveaux outils. Le rôle de la police est d'adapter le produit à ses besoins. Les technologies sont appropriées et adaptées par ses usagers. Dans l'esprit de cette nouvelle stratégie, la police est appelée à collaborer avec des experts et non plus à jouer le rôle d'experts comme elle le fait traditionnellement. Ainsi les policiers adaptent leurs méthodes de travail habituelles selon leur compétence propre aux outils performants qui leur sont proposés. Ajoutons toutefois, que si des tâches sont raffinées et simplifiées par les technologies, il peut en découler que le résultat final soit peu amélioré. Les nouvelles technologies ne créent pas la compétence ni l'expérience chez l'usager.

Les facteurs incitatifs et de blocage

Comment faciliter le passage aux technologies pour une organisation policière? Nogala (1993) identifie des forces motrices internes, des facteurs externes et des facteurs de blocage. Reprenons-les.

Les facteurs moteurs internes relèvent de facteurs de différents niveaux. Un premier porte sur l'amélioration des performances dans la mise en application de la loi et dans le travail de collaboration entre les services de police. Il s'agit autant de combattre le grand banditisme que les crimes au quotidien et les crimes technologiques en pleine expansion. Ces derniers constituent de nouveaux types de délits liés à l'usage des technologies et qui demeurent encore difficilement traités par les services de police. Conséquemment, les orientations et les stratégies retenues au sein de la police favorisent et accélèrent l'utilisation des technologies et lui donnent une place de plus en plus importante dans l'ensemble du système. Il reste des conditions essentielles à rencontrer à savoir avoir la capacité de payer, et la capacité de les intégrer dans le milieu du travail. Il s'agit aussi de renforcer la coopération entre les polices, coopération qui peut prendre la forme d'escouades spécialisées comme *Carcajou* mise sur pied pour combattre les bandes organisées de motards dans la région de Montréal au milieu des année 90 et qui rassemblait des policiers des services de la Sûreté du Québec, du Service de police de la Communauté urbaine de Montréal et de la Gendarmerie royale du Canada. Une telle coopération favorise des échanges rapides, une communication adéquate et le partage de plusieurs renseignements. Il reste à évaluer comment, dans les faits, se déroule le processus d'échange des renseignements surtout si les technologies de l'information ne sont pas compatibles.

Un second facteur s'inscrit dans un autre ordre d'idées. La police est définitivement engagée dans un processus de professionnalisation et de spécialisation des tâches. Les enquêteurs qui s'intéressent au crime organisé ont dû ajouter à leurs méthodes de travail la consultation du système automatisé de renseignements criminels (SARC II) qui permet de connaître la place et le rôle des criminels dans le crime organisé (Kerr, 1999b). Il en résulte que l'introduction de technologies de pointe et l'utilisation de toutes leurs possibilités demandent des qualifications techniques élevées et spécialisées. S'agit-il alors de former le personnel en place pour qu'il puise utiliser le potentiel des technologies, ou s'agit-il d'avoir des experts qui non seulement peuvent manipuler les technologies mais aussi être en mesure de suivre la progression rapide du changement dans ce domaine? Plus globalement, la vraie question demeure de savoir quelle est la vision stratégique que les services de police doivent développer pour répondre aux besoins des communautés qu'ils servent, pour rencontrer les besoins des membres à l'intérieur des services, et finalement, pour être capable de prendre des décisions éclairées quant au choix des technologies, choix qui ne deviennent pas obsolètes trop rapidement.

Enfin, un troisième facteur serait que les technologies apparaissent comme des armes efficaces qui détiennent des promesses de solutions inégalées. A cet effet, le *compstat*, par exemple, est devenu, suite à l'expérience de la police de la ville de New York (Bratton, Nobler, 1998), non seulement un outil stratégique de gestion des crimes par zones, mais en plus il sert à valoriser le rôle d'une police active autant dans la prévention que dans la répression (Green Mazerolle, Haas, 1998). Des séminaires avancés se donnent même sur le thème. De ce fait, la police est vue comme pouvant résoudre plus de problèmes et maintenir son pouvoir de contrôle social par les technologies devenues au service des communautés (National Institute of Justice, 1997).

Les facteurs incitatifs externes découlent du progrès technologique et de l'évolution sociale rapide. Un des éléments moteurs nouveaux et incontournables concernant les technologies tient au fait que le marché des technologies et le développement général évoluent à un rythme effarant (Castells, 1996). Le cycle des innovations devient court, les équipements plus puissants et plus abordables, les procédés complexes se transforment en outils courants. Il arrive qu'au bout de deux ou trois ans un système informatisé soit déjà dépassé ou encore qu'il ne soit plus compatible avec les autres systèmes informatiques acquis depuis l'installation initiale. En fin de compte les services de police risquent de se retrouver soit dépassés par le marché des technologies, soit en retard sur les plus récents développements, soit freinés dans leur évolution par le fait que des systèmes ne soient pas compatibles, soit limités dans leur expansion par le manque de ressources financières pour mettre à jour les systèmes en place Le marché des technologies arrive aux portes de la sécurité publique après avoir envahi la sécurité privée qui dépendra de moins en moins des personnes (Moore, 1995) comme nous l'avons déjà souligné. Par ailleurs, les besoins de sécurité des populations et les intérêts commerciaux privés font que des moyens de sécurité sont recherchés par des solutions technologiques (Boullier, 1993;Clarke, 1993). L'arrivée et l'implantation de la vidéo-surveillance ne demeure plus l'apanage de la sécurité privée mais devient un outil de travail pour des services de sécurité publique également (Ocqueteau, Pottier, 1993).

Les facteurs de blocage du progrès sont nombreux et portent sur plusieurs secteurs à la fois.

A partir de maintenant, la police aura recours de plus en plus à des équipements sophistiqués et coûteux. Or, il y a un net fossé entre le discours des ingénieurs et des spécialistes et l'expérience quotidienne des usagers dans la police. La technologie ne remplit pas toujours les fonctions promises ou n'apporte qu'un léger progrès. En fait, pour l'illustrer simplement, disons qu'on ne devient pas écrivain en utilisant un traitement de texte. Les technologies sont rendues performantes quand un certain nombre de conditions idéales sont remplies telles une formation adéquate, le support d'experts, des connaissances approfondies de l'usage de l'appareil. Quelques fois les technologies ne deviennent vraiment utiles qu'après de coûteuses adaptations pour les usagers.

Un autre facteur important et déterminant concerne les limites des ressources financières de la police. Il n'est pas possible de financer toutes les options techniques souhaitables et tous les produits vendus sur le marché. Les coûts directs et indirects sont élevés et récurrents. L'achat d'un appareil signifie désormais qu'à relativement court terme, soit quelques années, un nouvel appareil sera nécessaire et/ou son amélioration obligatoire. De même, le développement, la recherche et le maintien d'une expertise sont relativement coûteux pour la police, ce qui fait que très souvent les technologies ne sont pas vues ni perçues comme une priorité encore maintenant. De plus, une formation adaptée doit être développée et donnée à chaque évolution dans les technologies possédées par la police. Des coûts directs et immédiats en résultent. La police est entrée dans l'ère du paradigme de la permanence du changement.

Un autre aspect important du bouleversement créé par les technologies et qui devient un obstacle majeur mais complexe est la situation de la police au pays. Selon la constitution canadienne, la police relève de la juridiction des provinces à l'exception de la Gendarmerie royale du Canada. Il en découle une fragmentation de la police qui demeure difficile à combler quand vient le moment de développer des standards nationaux. De plus, il existe une grande disparité entre les services. Les services de police ne possèdent pas le réflexe de se rallier pour créer une masse critique pour l'achat de matériel par exemple. D'où les difficultés de rendre compatibles des technologies qui sont développées par des commerçants différents. Enfin, les services de petite et de moyenne taille n'ont pas d'experts parmi leurs employés réguliers pour évaluer les technologies, la pertinence des achats et pour assurer la planification stratégique des technologies à long terme (Brady, 1996).

Les coûts des technologies

Il est difficile de déterminer les coûts directs des technologies. Les coûts incluent-ils uniquement les appareils ou les logiciels, ou ne doivent-ils pas également intégrer les coûts reliés à la formation du personnel, au réaménagement des effectifs et à la sécurité des systèmes?

Il existe des coûts récurrents qui portent sur l'achat et la mise à jour des appareils et des outils technologiques de toutes sortes. Les budgets doivent donc être développés en conséquence. Il existe également les coûts cachés reliés à l'implantation des technologies. Ces coûts concernent les congés de

maladie à répétition ou prolongés de la part des individus qui résistent au changement ou qui veulent le saborder. Il y a aussi la démotivation et l'apathie qui se mesurent plus difficilement qui n'en demeurent pas moins des facteurs majeurs pouvant contribuer à l'échec d'une implantation et conséquemment engendrer des coûts élevés.

Une autre partie des coûts est attribuable à la formation des membres mais aussi des gestionnaires supérieurs. Dans l'un et l'autre cas les enjeux et les coûts de formation sont différents même si complémentaires. Il est remarquable de constater qu'il y a peu de littérature sur les questions de formation des gestionnaires de haut niveau par rapport aux technologies de l'information de même que sur les types de renseignements à fournir pour développer une vision stratégique et une prise de décision éclairée. Toutefois, la formation constitue une priorité constante et appelée à être réaménagée continuellement. Les programmes de formation de demain doivent être développés dans l'esprit des préoccupations et des besoins de demain. Encore ici une vision élargie doit illustrer les nouveaux enjeux que posent les technologies.

Enfin, la sécurité des technologies soulève aussi des problèmes majeurs et coûteux à résoudre comme à combattre. S'il est généralement admis que les technologies de l'information améliorent substantiellement l'efficacité et la performance des utilisateurs dans la police, comme nous le verrons plus loin, il est peut être moins connu, encore, qu'elles s'accompagnent d'une grande vulnérabilité (Grabosky, et al., 1996). Cette vulnérabilité s'illustre par les formes émergentes de nouveaux crimes comme la fraude par télémarketing, le détournement des transferts de fond, les interceptions illégales des téléphones cellulaires mais aussi le vandalisme électronique. Dans ce dernier cas, l'on parle de virus qui attaquent le système informatique tout comme des virus agressent l'humain ou l'animal. Des coûts énormes en découlent non seulement pour se préserver des attaques et invasions illégales mais également pour rétablir le système affaibli ou détruit (Bulletin sur la sécurité de l'informatique, 1998).

L'impact des technologies sur le fonctionnement de la police

Les impacts sont multiples et se reflètent différemment selon les secteurs touchés. Les impacts sont encore relativement difficile à décrire d'une facon spécifique. L'arrivée et l'usage des technologies de l'information influencent la facon d'organiser le travail technique, les facons de l'opérationnaliser et aussi les facons de l'évaluer. Le postulat de départ est le suivant: les technologies sont intégrées à la police à la lumière des effets bénéfiques qu'elles possèdent pour les opérations. Un tel postulat reste à être démontré. Dans le secteur des technologies de l'information en particulier on peut identifier trois grands ordres d'impacts.

Le recours à des technologies augmente l'efficacité dans le travail en éliminant ou en diminuant les répétitions dans des tâches surtout pour les patrouilleurs, d'où une augmentation du rendement, une réponse plus rapide et un taux de solution amélioré (Seaskate, 1998, Lingerfelt, 1996). On peut imaginer alors que les patrouilleurs ont davantage de temps à consacrer à la communauté par le déplacement d'une partie des tâches administratives vers du personnel non policier. Par ailleurs, dans le domaine de l'identité judiciaire, le fait d'accéder à des dossiers informatisés qui contiennent déjà des informations de base diminue beaucoup le temps pour compléter les formulaires informatisés. Il y a moins de répétitions dans les actions. De plus, les renseignements obtenus sont de meilleure qualité car les policiers peuvent procéder immédiatement à la vérification des banques de données et s'il y a lieu compléter les renseignements manquants.

Les technologies ouvrent la porte à la mise en place d'un réseau de communication étendu, performant et mettant en contact des services qui ne le seraient pas autrement. Toutefois il reste à évaluer la qualité des contacts entre les personnes et les résultats obtenus par les nouveaux réseaux. Une analyste d'un service de police de grande taille constatait qu'il lui était possible de rentrer en contact avec un grand nombre d'analystes et d'enquêteurs de son service grâce au courrier électronique et à l'internet. Toutefois, elle constatait aussi qu'un appel téléphonique permettait de développer des rapports plus concrets et plus personnalisés, ce qui favorisait l'échange de renseignements et une meilleure collaboration à long terme. Le contact direct de personne à personne repose sur le besoin de créer un vrai réseau par des contacts plus humains, lequel permet en retour d'obtenir des renseignements plus précis et spécifiques. Tandis que les renseignements plus généraux et factuels se transmettent bien par le

contact superficiel du courrier électronique.

La mise sur pied de réseaux de communication performants (ou importants) a un effet d'entraînement direct et immédiat qui transforme les pratiques de la prise de décision. En effet, il s'agit pour un service de police de pouvoir se connecter à un système puissant et performant, et pour ce faire, d'avoir les appareils compatibles avec les autres services ou avec les services de grande taille d'une région. Le transfert des connaissances et des renseignements colligés dans des banques de données passe de plus en plus aussi par le transfert des technologies. En ce sens les technologies de l'information deviennent des supports moteurs favorisant l'amélioration des techniques de travail. Elles ne les suppléent pas pour autant.

Le travail des policiers avec les technologies de l'information fait en sorte que la tâche est moins évaluée en terme de performance ou de produit quantitatif qu'en terme de résultats reflétés à travers les multiples connections à différents sites. Les nouvelles divisions du travail sont basées sur les capacités et les attributs d'un travailleur plutôt que sur la tâche. Par exemple, les équipes en identité judiciaire sont radicalement diminuées, mais le travail à exécuter est complété plus rapidement, plus efficacement, plus fidèlement tout en nécessitant beaucoup moins de personnel. Le travail d'un policier en identité judiciaire n'est pas nécessairement plus rapide qu'auparavant ce n'est pas nécessairement ce qui lui est demandé mais les résultats des tâches reliées à la section d'identité sont plus efficaces dans l'ensemble, car plusieurs des tâches répétitives ne sont plus accomplies avec l'arrivée des banques de données informatisées.

La formation

La formation des policiers se transforme avec l'arrivée des technologies. Non seulement un besoin pour former les individus à l'usage des technologies est éminent mais des technologies sont aussi utilisées pour offrir la formation. On parle ici du domaine en évolution de la formation à distance (Wells, Minor, 1998). Les personnes se forment selon leur besoin et par le biais de contacts électroniques dont internet (Myers, Myers, 1998) et à l'avenir intranet (Kerr, 1999a). Les individus peuvent avoir accès à la téléconférence, ou à des programmes de formation assistée par ordinateur ou par CD-rom (Hutchison et. Al. 1998), ou encore à des simulateurs pour le tir ou la conduite automobile pour confronter les apprenants à des situations le plus près possible du réel (Pilant, 1994). Une expérience canadienne dans le domaine de la formation est *Athabaska University*, une université virtuelle qui ne possède aucun campus où former ses étudiants.

A plusieurs reprises il a été mentionné que la formation devenait une priorité dans un contexte en mutation profonde comme l'est la police face aux technologies. En effet, les technologies font en sorte que les appareils et les banques de donnés sont plus puissantes, que la capacité d'échange des renseignements est décuplée et que les interconnections entre les systèmes, les services de police et les banques de données sont de plus en plus facilitées.

Le constat qui s'impose est le suivant: les technologies sont-elles en train de créer un nouveau métier de policier? De fait, un nouveau métier nécessitera du nouveau matériel qui commence à être intégré dans des services de police, un recrutement de personnel capable de répondre aux tâches de la police de demain et une formation qui puisse favoriser un usage optimum des outils qui seront offerts aux policiers. La formation deviendra nécessairement spécialisée et de haut niveau afin de comprendre le fonctionnement des technologies et de rencontrer les besoins des communautés, comme le gouvernement français le constatait lors des Assises nationales sur la formation qui se déroulaient au mois de février 1999 à Paris (France, 1999).

Des techniciens en informatique, des informaticiens, des spécialistes de systèmes sont appelés à faire partie des rangs de la police. Un service de police de petite taille comme le Service de police de Hull au Québec qui emploie une centaine de policiers a depuis cinq ans maintenant un informaticien comme employé permanent. Ce dernier gère les réseaux, planifie les changements à apporter à la technologie en place, relance le système en cas de dysfonctionnement, conçoit de nouvelles applications informatiques et assure l'administration de ce domaine. Il assure aussi que les systèmes rencontrent les critères de sécurité maximum pour protéger les renseignements du service de police. Il s'assure aussi que les systèmes sélectionnés par le service soient compatibles avec les différents services de police.

Les questions d'éthique et de responsabilité

Nulle part il n'est plus pertinent de se pencher sur un domaine à travers la loupe de l'éthique que l'usage des technologies. En effet, s'il est acquis depuis longtemps qu'un système informatique comme le Centre d'information de la police canadienne (CIPC) doit être protégé parce qu'il contient plusieurs renseignements sur les personnes, il devient prioritaire de s'assurer, à la lumière des possibilités de connexion et de rapidité des logiciels existants, que les policiers qui ont accès à ce type de banques de données autant pour son alimentation que pour y puiser des renseignements en respectent son usage exclusif (Marx, 1998). Dernièrement, une commission d'enquête révélait que des policiers avaient profité des données obtenues d'une banque informatisée à des fins personnelles (Commission d'enquête chargée de faire enquête sur la Sûreté du Québec,1998). Ce qui est inacceptable mais exceptionnel risque de devenir plus commun si une réflexion éthique sur les technologies et surtout sur leur usage n'est pas initiée et constamment alimentée. La technologie ne doit pas servir à des usages pour lesquels elle n'a pas été conçue. Il est bon de se rappeler que les questions d'éthique doivent faire partie du quotidien de tous les policiers quelque soit leur rang, leurs fonctions et le degré de leur ambition personnelle pour monter dans l'échelle de la hiérarchie policière. Une fois présentée dans une salle de classe, une approche éthique doit être maintenue et encouragée dans toutes les actions des policiers. A l'inverse, il serait souhaitable que les comportements non éthiques soient dénoncés, ce qui semble encore beaucoup trop difficile dans la culture policière.

Un autre enjeu porte sur les notions de responsabilités des services de police dans l'usage qu'ils font des technologies et les poursuites judiciaires qui peuvent en découler. L'arrivée d'armes non vulnérantes (non lethal weapon) comme le poivre de Cayenne (oléorésine capsicum), autorisées parce qu'elles représentent une alternative aux armes régulières, a entraîné aux Etats-Unis des poursuites qui se sont soldées par une condamnation des policiers qui en avaient fait usage avec un contrevenant difficile (Cansler, 1998). De même, l'interception de communications privées quand des clés en interdisent l'accès soulève à la fois le droit à la protection à la vie privée et le droit à la protection du public en général (Cansler, 1996). Il demeure que les technologies ne doivent pas être mal utilisée, ou encore utilisées à des fins qui ne leur étaient pas destinées.

Par ailleurs, on peut imaginer que les nouvelles méthodes de travail découlant d'appareils permettant de prendre les déclarations de prévenus sur les lieux du crime où dans l'auto-patrouille, comme cela se fait au Service de police de London en Ontario ou grâce à l'ordinateur portable contenant les formules adéquates, le prévenu confirme l'exactitude de la déclaration, à défaut de pouvoir y apposer sa signature, en appuyant sur le bouton d'envoi vers la banque de données au quartier général. On peut imaginer aussi que la galerie de photos (mug shot) qui permet une sélection formidable de suspects pour un crime pourra éventuellement poser des difficultés à la justice. Les photos digitalisées peuvent être modifiées par l'ordinateur sans laisser de traces. En d'autres mots, une photographie pourrait être aménagée pour rencontrer les caractéristiques d'un suspect afin qu'elle lui corresponde. Par cet exemple banal et presque farfelu, nous voulons souligner que le travail de la police se simplifie et se raffine grâce à la technologie. Il reste à voir comment le droit réagira à l'implantation de ces nouveaux moyens.

Enfin, l'encryptage devient une question majeure qui soulève des interrogations de fond. L'encryptage est la capacité de cacher le contenu des message en les rendant incompréhensibles sauf aux récipiendaires autorisés. Il est connu qu'internet a été financé par l'armée américaine durant la guerre froide pour multiplier les sources de communication en cas d'attaque nucléaire majeure. Ce système constituant un très vaste réseau d'ordinateurs à travers le monde (on estimait à environ 80 000 réseaux d'ordinateurs indépendants en 1997 (Dobeck, 1997)) devient relativement difficile à pénétrer par les services de mise en application de la loi. Une des solutions proposées aux Etats Unis est que le gouvernement exerce un contrôle sur les serveurs, proposition qui ne fait pas l'unanimité et qui contrevient au principe même d'Internet et du droit à la vie privée (Pilant, 1999).

Remarques concluantes

Un grand nombre de facteurs médiatisant le rôle de la technologie dans la police relèvent en grande partie des forces sociales dont l'interaction et l'évolution ne sont pas aisément prédictibles. Un directeur motivé

par les technologies, des spécialistes qui font avancer les dossiers, des budgets qui sont développés à la lumière de pressions de champions aguerris, le futur des technologies, tout cela repose sur des considérations strictement humaines. Les technologies sont à la portée de la main, il reste aux preneurs de décision à le comprendre.

Déjà, des études portent sur comment des services de police colligent et analysent les données (types, buts, etc.) et comment aussi des policiers y ont accès (O'Shea, 1998). D'autres essaient de voir à quel point les technologies diminuent le nombre de rapports et de formulaires à compléter (Moriarty, Dover, 1998). D'autres encore montrent à la suite de sondages auprès de groupes cibles, que les crimes par informatique(copie d'un logiciel, vente illégale, accès illégal par des hackers) ne sont pas nécessairement vus comme des crimes, surtout de la part d'étudiants en génie ou en technologie (Mercier, 1998).

Si, comme nous l'avons constaté, la mise en place des outils technologiques nécessite une planification en terme de coûts et de modification des fonctions, il demeure que le développement des outils se fait à un rythme effréné et que le commerce de ces outils se produit de la même façon. D'une part, les policiers réclament de leurs patrons des appareils qui facilitent et améliorent la tâche. D'autre part, les patrons sont sollicités par le marché qui leur soumet les bénéfices et les avantages des outils développés, avantages qui dépassent quelques fois les besoins réels des services ou créent de nouveaux coûts d'implantation par l'incompatibilité des systèmes.

Or, il n'existe pas une rationalité dans l'intégration, ni dans l'usage des technologies. Notre hypothèse est qu'une rationalité ponctuelle appuyée par un savoir qui demeure extérieur et incontrôlable à la police soutient la prise de décision. La méconnaissance des outils conduit à leur intégration partielle ou superficielle pour tenter de rendre compatible le nouvel outil avec les méthodes de travail traditionnelles. En fin de compte, les technologies passent par une phase transitoire obligée où la police doit apprendre d'abord à apprivoiser l'arrivée d'outils prometteurs d'efficacité dans la solution des problèmes avant de les intégrer et de les manipuler correctement. Il reste à s'assurer de ne pas développer de dépendance trop forte par rapport aux fournisseurs et aux contrôleurs du marché (Naulleau, 1998). Une fois cette phase transitoire complétée, elle peut s'avérer relativement longue compte tenu de facteurs humains et budgétaires en jeu. Il reste à apprendre à l'intégrer aux méthodes de travail habituelles, connues et développées pour une police d'une autre époque. Dû au fait qu'une formation adaptée doit être offerte, que des experts doivent être sur place ou facilement disponibles pour aider ou pour manipuler les appareils et qu'une réorganisation des ressources humaines a été nécessaire, l'intégration se fait comme le jeu du saut au mouton, des hauts et des bas et des entre deux.

Non seulement faut-il préparer les services de police à comprendre les grands bouleversements provoqués par l'arrivée d'outils technologiques performants et complètement nouveaux pour le domaine policier, mais en plus, il faut les préparer à intégrer les outils, à les manipuler correctement de sorte que la police ne devienne pas dépassée par les nouvelles formes de criminalité issues des technologies, mais également par la criminalité plus traditionnelle. S'il est relativement facile de comprendre que les fraudes par l'informatique nécessitent des expertises de pointe et des connaissances spécialisées, il faut aussi se rappeler que le contrôle du crime passera aussi par des outils nouveaux comme la télédétection (Quirion, Lamy, 1999) et qui demandent à être apprivoisé par les policiers en fonction.

Références

Akrich, M.; Méadel, C. (1993). Technologies de sécurité et organisation. *Les Cahiers de la sécurité intérieure*,21:53-59.

Anderson, P. B. (1997). Web Technology in Law Enforcement. Page web consultée le 1999-4-26.

Audet, M.; Jacob, R.; Lauzon, N.; Rondeau, A. (1996). *Renouvellement des services publics et autoroute de l'information: vers un modèle stratégique de transformation et de critères d'aide à la décision.* Version finale. Présenté au Centre francophone de recherche en informatisation des organisaitons (CEFRIO). Septembre.

Boullier, D. (1993). La vidéosurveillance à la RATP: un maillon controversé de la chaîne de production de sécurité. *Les Cahiers de la sécurité intérieure*, 21:88-100.

Brady, T. (1996). The Evolution of Police Technology. In National Institute of Justice, Office of Community Oriented Policing Services (ed) *Technology for Community Policing.* Conference Report. National Institute of Justice.

Bratton, W.; Nobler, P. (1998). Turn Around. How America's Top Cop Reversed the Crime Epidemic. New York: Random House.

Breton, P. (1966). L'informaticien et la sécurité: enquête sur un antagonisme. *Les Cahiers de la sécurité intérieure*, Entreprise et sécurité, 24:36-47.

Bulletin sur la sécurité de l'informatique. (1998). Sous-direction de la sécurité des technologies de l'information, GRC. Sécurité des TI. Janvier. No 45.

Campbell, F. (1997). High-Tech Advances Bring New Tools. *Police*, 21, 10:60-63.

Cansler, R. (1996). Technology Liability Considerations. In National Institute of Justice, Office of Community Oriented Policing Services (ed) *Technology for Community Policing.* Conference Report. National Institute of Justice.

Cansler, R.E. (1998). Technology Liability Considerations. *The police Chief*, May:53-55.

Carpenter, G. (1984). Preliminary Considerations for the Impact of Microtechnology on Police Management. *Canadian Police College Journal*, 8, 2:93-106.

Carter, D.; Katz, A. (998). Computer Applications by International Organized Crime Groups. In L. Moriarty; D. Carter (eds.) *Criminal Justice Technology in the 21st Century.* Springfield: Charles C. Thomas.

Castells, M. (1996). *The Rise of the Network Society.* The Information Age: Economy, Society and Culture. Volume I. Great Britain; Blackwell.

Catalyst (1996). Denver Partnerships Produce Unexpected Evidence, 16, 2:1-2.

Clarke, R. (1993). Les technologies de la prévention situationnelle. *Les Cahiers de la sécurité intérieure*, 21:101-112.

Commission d'enquête chargée de faire enquête sur la Sûreté du Québec. (1998). *Rapport de la Commission d'enquête chargée de faire enquête sur la Sûreté du Québec. Pour une police au service de l'intégrité et de la justice.* Volume, I, 2, Sommaire et recommandations, Annexes. Commission L. Poitras. Québec: Les Publications du Québec.

Corsentino, D.; Pettinari, D. (1996). A Fork in the Road. *Sheriff,* March-April:1012, 35.

Coutorie, L. E. (1995). The Future of High-Technology Crime: A Parallel Delphi Study. *Journal of Criminal Justice*, 233, 1:13-27.

Dobeck, M. (1997). Taking Advantage of the Internet. *The Police Chief*, January:35-38.

Dorn, N. (1998). Du renseignement au partage des informations: l'intelligence protéiforme. *Les Cahiers de la sécurité intérieure*, 34:91-108.

Ericson, R.; Haggerty, K. (1997). *Policing the Risk Society*. Toronto: University of Toronto Press.

France, Ministère de l'Intérieur (1999). Assises de la formation et de la recherche dans la police nationale (1999). Table ronde no 2: former à l'utilisation des technologies nouvelles. Paris: La Villette.

Fulton, R. (1995). When Law Enforcement Met Industry, Transferring Military Technology. *Law Enforcement Technology*, September:56-60.

Galland, J.P. (1996). Eléments pour une prospective de la sécurité. *Les cahiers de la sécurité intérieure*, 24, Deuxième trimestre:85-102.

Goodman, M.D. (1997). Working the Net. Exploiting Technology to Increase Community Involvement and Enhance Service Delivery. *The Police Chief*, August:45-53.

Grabosky, P. ; Smith, R.; Wright, P. (1996). Crime and Telecommunications. Trends and Issues. *Crime and Criminal Justice*, 59: .

Green Mazerolle, L. ; Haas, R. (1998). "The problem Solver". The Development of Information Technology to Support Problem-Oriented Policing. In L. Moriarty; D. Carter (eds.) *Criminal Justice Technology in the 21st Century*. Springfield: Charles C. Thomas.

Haley, K.; Taylor, R. (1998). Police Stations in Cyberspace: A Content Analysis of Law Enforcement Agency Home Pages. In L. Moriarty; D. Carter (eds.) *Criminal Justice Technology in the 21st Century*. Springfield: Charles C. Thomas.

Hutchison, J.; Mays, J.; Moriarty, L. (1998). Teaching Statistics in the 21st Century: Technology in the Classroom. In L. Moriarty; D. Carter (eds.) *Criminal Justice Technology in the 21st Century*. Springfield: Charles C. Thomas.

Johnson, R. (1997). High-Tech Help. Robots Lend a Hand in the Labs. *Pony Express*, December: 18-19.

Kerr, J. (1999a). Inside the Web. Intranet Pilot Project Keeps the Force Connected. *Pony Express*, January-February: 7.

Kerr, J. (1999b). Making Connections, Computer Database Helps Investigators Piece Organized Crime Networks Together. *Pony Express*, January-February:16.

LeBeuf, M.E. (1998). *Police et citoyens - des liens à redéfinir*. Ottawa: Centre de recherche. Collège canadien de police.

LeBeuf, M. E. (1999). Police de proximité et contrats locaux de sécurité- Que retenir du modèle canadien de police communautaire? Rapport présenté à l'Institut des Hautes Etudes de la Securité Intérieure-IHESI. Janvier.

Lingerfelt, J. (1996). Technology as a Force Multiplier. In National Institute of Justice, Office of Community Oriented Policing Services (ed) *Technology for Community Policing*. Conference Report. National Institute of Justice.

Loree, D. (1987). Technological Innovation and Social Control: Some Implications for Police. *Canadian Police College Journal*, 11, 1:13-33.

MacDonald, V.; Martin, M.(1986). Specialists and the Personnel Structures of Canadian Police Forces. *Canadian Police College Journal*, 10, 3:189-226.

Manning, P. (1992). Technological and Material Resource Issues. In L. T. Hoover (ed.) *Police Management Issues & Perspectives*.

Martin, S. (1996). *The Impact of Information Technology Upon the Traditional Hierarchical Structures in Highly Bureaucratic Organizations*. Command College Class XXI. Peace Officer Standards and Training. Sacramento, California.

Marx, G. (1997). The Declining Significance of Traditional Borders (and the Appearance of New Borders) in an Age of High Technology. In P. Drogue (ed.) *Intelligent Environments*.

Elsevier Science.

Marx, G. (1998). An Ethics For The New Surveillance. Page web consultée le 1998-10-2.

McLean-Lipinski, J.R. (1999). Enhancing the Use of Tehcnology in Law Enforcement. Page web consultée le 1999-05-06.

Mercier, P. (1998). On-Line Crime: In Pursuit of Cyber Thieves. In L. Moriarty; D. Carter (eds.) *Criminal Justice Technology in the 21st Century*. Springfield: Charles C. Thomas.

Moore, R.H. (1995). Technology and Private Security; What Does the Future Hold? Journal of Security Administration,.18,2:1-9.

Moriarty, L.; Dover, T. (1998). The Centralized Data Entry (CDE) System: One County's Attempt at Managing Burdensome Paperwork with Innovative Technology. In L. Moriarty; D. Carter (eds.) *Criminal Justice Technology in the 21st Century*. Springfield: Charles C. Thomas.

Morrison, R. (1996). Information Technology 2000. What's Ahead in the 21st Century. *Law Enforcement Technology*, June:40-43.

Myers, L.; Myers, L. (1998). Integrating Computers in the Classroom: A National Survey of Criminal Jusitice Educators. In L. Moriarty; D. Carter (eds.) *Criminal Justice Technology in the 21st Century*. Springfield: Charles C. Thomas.

National Institute of Justice (1994). *25 Years of Criminal Justice Research*. National Institute of Justice. December.

National Institute of Justice (1997). *Technology for Community Policing*. Conference Report. Sponsored by National Institute of Justice, Office of Community Oriented Policing Services, National Institute of Justice. June.

Naulleau, D. (1998). Le bogue de l'an 2000: un révélateur de la vulnérabilité de nos libertés. *Les Cahiers de la sécurité intérieure*, 34:69-90.

Nogala, D. (1993). Le rôle de la technologie dans la police de demain. *Les cahiers de la sécurité intérieure*, 14, août-octobre:137-158.

O'Shea, T. (1998). Analyzing Police Department Data: How and How Well Police Officers and POlice Departments Manage the Data They Collect. In L. Moriarty; D. Carter (eds.) *Criminal Justice Technology in the 21st Century*. Springfield: Charles C. Thomas.

Ocqueteau, F.; Pottier, M.L. (1993). Vidéosurveillance et gestion de l'insécurité dans un centre commercial: les leçons de l'observation. *Les Cahiers de la sécurité intérieure, 21:60-74.*

Parsons, S. L. (1993). Technology Can Boost Safety in the Field. *Police and Security News*, 9,4:19-22,27.

Pilant, L. (1999) The Debate Over Encryption. *The Police Chief*, LXVI, 1:31-35.

Pilant, L. (1994). Spotlight on High-Tech Training. *The Police Chief*, July: 25, 27-33.

Pitcher, P. (1995). *Artist, Crafstmen and Technocrats: the Dreams, Realities and Illusions of Leadership*. Toronto: Stoddart.

Preimsberger, D. (1996). Cops and Space Scientist:New Crime-Fighting Partners. *The Police Chief*, October:108-114.

Quirion, S.; Lamy, O. (1999) La télédétection appliquée aux cultures agricoles et illicites. Sommets, 13, 2:22.

Rodriguez, M. (1995). An Overview of Law Enforcement Technology. *The Police Chief*, April: 15-29.

Rosé, P. (1996). L'informaticien et la sécurité de l'entreprise. *Les cahiers de la sécurité intérieure*, 24: 25-35.

Seaskaste, Inc. (1998). *The Evolution and Development of Police Technology*. A technical Report prepared for The National Committee on Criminal Justice Technology. National Institute of Justice.

Sheptycki, J. (1998). Reflections on the Transnationalization of Policing; the Case of the RCMP and Serial Killers. *International Journal of the Sociology of Law*, 26:17-34.

Sloan, R.C. (1997). How Can Technology Help Police Be More Effective in Community Policing? In National Institute of Justice, Office of Community Oriented Policing Services (ed) *Technology for Community Policing*. Conference Report. National Institute of Justice.

Smietan, I.; Ferris, D. (1996). Detecting Concealed Weapons. In National Institute of Justice, Office of Community Oriented Policing Services (ed) *Technology for Community Policing*. Conference Report. National Institute of Justice.

Soullière, N. (1999). Police et technologies: un bilan historique, un regard contemporain. Ottawa: Collège canadien de police, Centre de recherche.

Strandberg, K. (1998). Websites For Law Enforcement. *Law Enforcement Technology*, January:59-60.

Tafoya, W. (1997). Policing High Tech Crime. *Crime & Justice*, October, 23.

Wells, J.; Minor, K. (1998). Criminal Justice Students' Attitudes Toward Distance Learning as a Function of Demographics. In L. Moriarty; D. Carter (eds.) *Criminal Justice Technology in the 21st Century*. Springfield: Charles C. Thomas.

Wilsker, I. (1997). Cops on the Web. In National Institute of Justice, Office of Community Oriented Policing Services (ed) *Technology for Community Policing*. Conference Report. National Institute of Justice.